

RATIONAL RIGIDITY FOR $F_4(p)$

ROBERT GURALNICK, FRANK LÜBECK, AND JUN YU

ABSTRACT. We prove the existence of certain rationally rigid triples in $F_4(p)$ for good primes p (i.e., $p > 3$), thereby showing that these groups occur as regular Galois groups over $\mathbb{Q}(t)$ and so also over \mathbb{Q} . We show that these triples give rise to rigid triples in the algebraic group and prove that they generate an interesting subgroup in characteristic 0.

1. INTRODUCTION

The question on which finite groups occur as Galois groups over the field of rational numbers is still widely open. Even if one restricts to the case of finite non-abelian simple groups, only rather few types have been realized as Galois groups over \mathbb{Q} . These include the alternating groups, the sporadic groups apart from M_{23} , and some families of groups of Lie type, but even over fields of prime order mostly with additional congruence conditions on the characteristic. In the present paper we show that $F_4(p)$ occur as Galois groups over \mathbb{Q} for all good primes p . In [7], a similar result was proved by Guralnick and Malle for $E_8(p)$. A similar result has been proved for $G_2(p)$ for $p > 5$ in [5] and for $p = 5$ in [19].

See [7] and more generally [15] for more on the general problem of producing Galois groups over \mathbb{Q} . In the last few years different approaches produced Galois groups over \mathbb{Q} (but not necessarily regular Galois extensions of $\mathbb{Q}(t)$; such extensions are produced by the rigidity method). See in particular [9, 10, 20, 21].

Our proof relies on the well-known rigidity criterion of Belyi, Fried, Matzat and Thompson. In addition, we use results about subgroups of a simple linear algebraic group of type F_4 which contain regular unipotent elements (in particular results from [16, 7]).

Let $p > 3$ be a prime and k be an algebraic closure of the finite field \mathbb{F}_p with p elements. Set $G = F_4(k)$. We consider three conjugacy classes C_1, C_2 and C_3 in G . Here C_1 is the conjugacy class of involutions with centralizer of type $A_1 + C_3$, and C_2 is the conjugacy class of elements of order $2p$ where the 2-part has a centralizer of type B_4 and the unipotent part is a long root element in that centralizer. Finally C_3 is the class of regular unipotent elements.

All classes have representatives in the finite subgroup $F_4(p)$ over the prime field. And since $p > 3$, all centralizers of elements in these classes are connected (see section 3 for details). In particular, for each finite subgroup $F_4(q)$, q any power of p , the intersection $C_i(q) := C_i \cap F_4(q)$ ($1 \leq i \leq 3$) is a single $F_4(q)$ -conjugacy class.

Furthermore, the classes $C_i(q)$ are rational, that is for any $g \in C_i(q)$ and $k \in \mathbb{Z}$ prime to the order of g we have $g^k \in C_i(q)$. (Let $g = su = us \in C_i(q)$ with s semisimple and u

Date: December 8, 2015.

2000 Mathematics Subject Classification. Primary 12F12, 20C33; Secondary 20E28.

Key words and phrases. Inverse Galois problem, rigidity, Lie primitive subgroups, regular unipotent elements.

Robert Guralnick was partially supported by the NSF grants FRG-1265297 and DMS-1302886. He also thanks the Simons Foundation for its support. This work was initiated in Spring 2013 when Robert Guralnick and Jun Yu were visiting the Institute for Advanced Study. They thank the Institute for its hospitality and support.

unipotent. Then $s^k = s$ because the order of s is 1 or 2, and u^k is conjugate to u in the centralizer of s in $F_4(q)$ because the class of u in that centralizer is uniquely determined by its size.)

We consider the variety

$$V(C_1, C_2, C_3) = \{(x, y, z) \in C_1 \times C_2 \times C_3 \mid xyz = 1\} \subset G^3,$$

on which G acts by componentwise conjugation.

Our main result is as follows.

Theorem 1.1. *Let $p, k, G = F_4(k), X := V(C_1, C_2, C_3)$ be as above. Then G has a single regular orbit on X and if $(x, y, z) \in X$, then $\langle x, y \rangle \cong F_4(p)$. Moreover, for any power q of p the subgroup $F_4(q)$ has a single regular orbit on $X(q)$, the \mathbb{F}_q -rational points of X .*

As noted the rigidity criterion as stated in [15, I. Thm. 4.8] implies the following (we use that the center of $F_4(p)$ is trivial, and that the classes $C_i(p)$ are rational).

Corollary 1.2. *If $p > 3$ is a prime, then $F_4(p)$ is a regular Galois group over $\mathbb{Q}(t)$ and in particular is a Galois group over \mathbb{Q} .*

Remark. This result was already obtained for $p \geq 19$ and $p \equiv 2, 6, 7$ or $11 \pmod{13}$ in [14], using a similar argument for a different triple of conjugacy classes.

As usual for applications of the rigidity criterion our proof has two main parts. In section 2 we show that any triple in $V(C_1, C_2, C_3)$ generates a subgroup which contains a conjugate of $F_4(p)$. We use non-trivial results on maximal subgroups of G containing a regular unipotent element and some representation theory for Levi subgroups of G .

In section 3 we compute a certain estimate for the structure constants of the class triples $C_i(q)$ ($1 \leq i \leq 3$) for all powers q of p . We use Deligne-Lusztig theory for these computations. These computations are a bit more complicated than, e.g., in [7] because many character values on the mixed class $C_2(q)$ are needed.

In section 4 we combine the results and prove Theorem 1.1.

Since $G = F_4(k)$ has a single regular orbit on $V(C_1, C_2, C_3)$ for k algebraically closed of good positive characteristic, it follows that the same is true if k is an algebraically closed field of characteristic 0. Precisely as in [7] since $C_G(z)$ for $z \in C_3$ is an affine space of dimension 4, it follows that this torsor is trivial and so G has a single orbit on the k -points of the variety described above over any field of characteristic $p \neq 2, 3$ (including characteristic zero).

Arguing exactly as in [7], we can also produce such triples over $G(\mathbb{Z}_p)$ and so deduce:

Theorem 1.3. *Let k be an algebraically closed field of characteristic 0. Let $G = F_4(k)$ and C_i , $1 \leq i \leq 3$, be the conjugacy classes described above. Let $X := V(C_1, C_2, C_3)$. For a triple $c \in X$, let $\Gamma(c)$ denote the group generated by c .*

- (1) *For any $c \in X$, $\Gamma(c)$ is Zariski dense in G .*
- (2) *If k_0 is a subfield of k , then $X(k_0)$, the k_0 -rational points of X , is a single $F_4(k_0)$ -orbit (where $F_4(k_0)$ is the split group over k_0).*
- (3) *Set $R = \mathbb{Z}[1/6]$. There exists $c \in X(R)$ such that $\Gamma(c) \leq F_4(R)$ and surjects onto $F_4(R/pR)$ for any good prime p . In particular, $\Gamma(c)$ is dense in $F_4(\mathbb{Z}_p)$ with respect to the p -adic topology for any good prime p .*

We thank Zhiwei Yun for suggesting the conjugacy classes considered in this paper (see also the discussion in [7, 7.]).

2. A GENERATION RESULT

Fix a prime $p > 3$ and let k be an algebraic closure of \mathbb{F}_p . Let $G = F_4(k)$ and let C_i , $1 \leq i \leq 3$, be the conjugacy classes of G described in the introduction.

Theorem 2.1. *If $(x, y, z) \in V(C_1, C_2, C_3)$, then $H := \langle x, y, z \rangle$ contains a conjugate of $F_4(p) \leq F_4(k)$.*

Remark. In section 4 we will show, using theorem 3.1, that in fact H is a conjugate of $F_4(p)$.

Proof. (of the theorem)

(1) Let $y = y_s y_u = y_u y_s$ with y_s semisimple and y_u unipotent be the Jordan decomposition of y . Since y_s and y_u are powers of y we know that H contains two involutions x and y_s which are not conjugate and two unipotent elements y_u and z which are not conjugate in $F_4(k)$.

(2) The finite maximal subgroups of $F_4(k)$ which contain a regular unipotent element which do not contain a conjugate of $F_4(p)$ and are also not contained in any proper positive dimensional subgroup (called *Lie primitive* subgroups) were determined in [7, Theorem 3.4(a)]. These subgroups have the property that p' -powers of any non-trivial unipotent element yield representatives of all their non-trivial unipotent conjugacy classes. Hence all unipotent elements in these subgroups are regular unipotent in $F_4(k)$ and so they cannot contain H .

(3) The maximal closed subgroups of $F_4(k)$ of positive dimension which contain a regular unipotent element were determined in [16, Theorem A]. These are parabolic or reductive of type A_1 (note that we assume $p > 3$). It is clear that H cannot be contained in a subgroup of type A_1 which contains only one class of unipotent elements. In the remainder of this proof we show that H also cannot be contained in any proper parabolic subgroup of G .

(4) Let $P < G$ be a maximal parabolic subgroup and assume $H = \langle x, y, z \rangle \leq P$. Let $U \triangleleft P$ be the unipotent radical of P and L a Levi complement. So, $P = U \rtimes L$. Every element $g \in P$ can be uniquely written as $g = g' \bar{g}$ with $g' \in U$ and $\bar{g} \in L$ and we have a homomorphism $P \rightarrow L$, $g \mapsto \bar{g}$, which maps semisimple elements to semisimple elements and unipotent elements to unipotent elements.

For the involution $x = x' \bar{x}$ we get that \bar{x} also has order 2 and that $x \bar{x} = x'$ is unipotent and so of odd order. Hence x and \bar{x} are conjugate in the dihedral group they generate and so in G . The same argument shows that y_s and \bar{y}_s are conjugate involutions in G .

To find the possibilities for \bar{y}_u we use the fact that for any unipotent element $u \in P$ the element \bar{u} is contained in the closure of the G -conjugacy class u^G , see [12, (9.5.2)]. Using this and [3, 13.4], it follows that \bar{y}_u is trivial or is conjugate to a long root element in G .

The relation $xyz = 1$ implies $\bar{x} \bar{y}_s \bar{y}_u \bar{z} = 1$.

Our strategy is to find a representation of L such that we can show that $\bar{x} \bar{y}_s \bar{y}_u$ has an eigenvalue -1 which is in contradiction to \bar{z}^{-1} being unipotent. Note that in fact \bar{z} is a regular unipotent element in L (we will not use this though).

(5) We use the setup described in [2, Section 2] to determine classes of involutions in G and some Levi subgroups, and to compute the eigenvalues of involutions in various representations.

The group G can be described by k and a root datum (X, R, Y, R^\vee) . Here X and Y are dual \mathbb{Z} -lattices of rank 4. As \mathbb{Z} -basis of Y we choose a set of simple coroots in R^\vee (note that G is simply-connected). The dual basis of X consists of the fundamental weights of G and the corresponding set of simple roots with respect to this basis is given by the transposed

Cartan matrix of the root system of G , that is the rows of $\begin{pmatrix} 2 & -1 & 0 & 0 \\ -1 & 2 & -2 & 0 \\ 0 & -1 & 2 & -1 \\ 0 & 0 & -1 & 2 \end{pmatrix}$ (the first

two simple roots are long). From this it is straightforward to write down matrices for the Coxeter generators of the Weyl group W of G acting on X : $s_\alpha(x) = x - \langle x, \alpha^\vee \rangle \alpha$, where α is a simple root, α^\vee the corresponding coroot, and $\langle \cdot, \cdot \rangle$ is the pairing between X and Y . Similarly, matrices for the Weyl group generators acting on Y can be computed.

This also describes the action of the Weyl group W on a maximal torus of G which is isomorphic to $T = Y \otimes_{\mathbb{Z}} (\mathbb{Q}/\mathbb{Z})_{p'}$. A torus element $t = (t_1, t_2, t_3, t_4) \in T$ can be evaluated at a weight $x = (x_1, x_2, x_3, x_4) \in X$ by $\sum_{i=1}^4 x_i t_i \in (\mathbb{Q}/\mathbb{Z})_{p'} \cong k^\times$. The roots which have t in their kernel form the root system of the centralizer of t .

Conjugacy classes of semisimple elements are in bijection with W -orbits in T (see [3, 3.7]). Computing the W -orbits on the 15 elements of order 2 in T , we recover the 2 conjugacy classes of involutions in G (the class of x with centralizer of type $A_1 + C_3$ and the class of y_s with centralizer of type B_4) and all their representatives in T . We will use this below to find the fusion of classes of involutions in Levi subgroups into G .

Let L_i ($1 \leq i \leq 4$) be the standard Levi subgroups of G , whose root datum we get from the root datum of G by removing the i -th simple root and the corresponding coroot. We denote by P_i the corresponding maximal standard parabolic subgroup and U_i its unipotent radical. The derived subgroup L'_i of L_i is also of simply-connected type and the intersection of $T \cap L'_i$ consists of the $t = (t_1, t_2, t_3, t_4)$ with $t_i = 0$ (see [2, 2.6]). We now consider each P_i separately¹

(6) Case P_1 . The commutator subgroup L'_1 is isomorphic to $\mathrm{Sp}_6(k)$. We consider $\bar{x}\bar{y}_s\bar{y}_u\bar{z} = 1$. The only unipotent class of L_i (or L'_i) which is conjugate in G to a long root element is the class of a long root element in L'_1 (see the description of unipotent classes in [3, 13.1] which also holds in characteristic > 3). So, \bar{y}_u is trivial or a long root element in L'_1 .

Using the Weyl group of L_1 to compute its orbits on the involutions in T we see that L_1 has one class of involutions which are conjugate to y_s in G and three classes of involutions which are conjugate to x in G . Only one of the classes conjugate to x is not contained in L'_1 . Since $\bar{x}\bar{y}_s\bar{y}_u\bar{z} = 1$ and \bar{y}_s and the unipotent elements \bar{y}_u and \bar{z} are in L'_1 it follows that \bar{x} must also lie in L'_1 .

We consider the irreducible representation of L_1 with highest weight $(0, 0, 0, 1)$. This is an extension of the 6-dimensional natural representation of L'_1 to L_1 (compare [2, 3.5 and 3.6(a)]). Its weights consist of the W -orbit of $(0, 0, 0, 1)$.

The image of \bar{y}_u is trivial or has a unique non-trivial Jordan block of size 2; in any case \bar{y}_u has at least a 5-dimensional 1-eigenspace. From the weights and class representatives we compute that \bar{y}_s has a 2-dimensional 1-eigenspace and a 4-dimensional (-1) -eigenspace. For \bar{x} there are two possibilities, it has eigenvalue (-1) either on the full space or on a

¹Using an approach in [1, Section 3.1], we can describe the isomorphism type of each L_i ($1 \leq i \leq 4$). Precisely we have

$$\begin{aligned} L_1 &\cong (\mathrm{Sp}_6(k) \times k^*) / \langle (-I, -1) \rangle, \\ L_2 \cong L_3 &\cong (\mathrm{SL}_3(k) \times \mathrm{SL}_2(k) \times k^*) / \langle (\omega I, I, \omega^{-1}), (I, -I, -1) \rangle, \\ L_4 &\cong (\mathrm{Spin}_7(k) \times k^*) / \langle (-1, -1) \rangle. \end{aligned}$$

By [8, Table 2], the centralizer of x is a subgroup isomorphic to $(\mathrm{Sp}_6(k) \times \mathrm{SL}_2(k)) / \langle (-I, -I) \rangle$, which contains a conjugate of L_1 ; the centralizer of y_s is a subgroup isomorphic to $\mathrm{Spin}_9(k)$, which contains a conjugate of L_4 . Then, using the description of fusions of involutions in these symmetric subgroups (pages 414-415 in [8, Table 2]), we can also identify the possible classes of \bar{x} and \bar{y}_s in L_1 (or L_4). By describing the fusion of involutions in a connected semisimple subgroup of G which is isomorphic to $(\mathrm{SL}_3(k) \times \mathrm{SL}_3(k)) / \langle (-I, -I) \rangle$, we can also identify the possible classes of \bar{x} and \bar{y}_s in L_2 (or L_3).

2-dimensional subspace. In any case we find that $\bar{x}\bar{y}_s$ has at least a 2-dimensional (-1) -eigenspace and so $\bar{x}\bar{y}_s\bar{y}_u$ has at least a 1-dimensional (-1) -eigenspace. On the other hand \bar{z} is unipotent and has no eigenvalue (-1) . This shows that H cannot be contained in P_1 .

(7) Case P_2 . Here L'_2 is isomorphic to $\mathrm{SL}_2(k) \times \mathrm{SL}_3(k)$ and only the nontrivial unipotent elements in the $\mathrm{SL}_2(k)$ -component are conjugate to y_u in G . We consider the representation of L_2 with highest weight $(1, 0, 0, 0)$ which is an extension of the natural 2-dimensional representation of the $\mathrm{SL}_2(k)$ -component of L'_2 .

The group L_2 contains only one class of involutions conjugate to y_s in G , this is contained in L'_2 and its elements act as identity on the 2-dimensional representation. Since $\bar{x}\bar{y}_s\bar{y}_u\bar{z} = 1$ and \bar{y}_s and the unipotent elements \bar{y}_u and \bar{z} are in L'_2 it follows that \bar{x} must also lie in L'_2 .

There are four classes of L_2 which belong to the class of x in G , two of them are in L'_2 and so may contain \bar{x} . In both cases \bar{x} acts as (-1) times the identity on the 2-dimensional representation. We get that the image of $\bar{x}\bar{y}_s\bar{y}_u$ has eigenvalue (-1) in this 2-dimensional representation. This is not possible because \bar{z} is unipotent.

(8) Case P_3 . Here L'_3 is isomorphic to $\mathrm{SL}_3(k) \times \mathrm{SL}_2(k)$ and only the root elements of the $\mathrm{SL}_3(k)$ -component are conjugate to y_u in G . We consider the representation of L_3 with highest weight $(1, 0, 0, 0)$ which extends the 3-dimensional natural representation of the $\mathrm{SL}_3(k)$ -component of L'_3 . We find that for all possibilities \bar{y}_s acts trivially in this representation and the image of \bar{x} has a (-1) -eigenspace of dimension 2. Furthermore, the image of \bar{y}_u has at most one Jordan block of size 2. This leads to a contradiction as in the previous cases.

(9) Case P_4 . Now L'_4 is isomorphic to a spin group $\mathrm{Spin}_7(k)$. We proceed as in the other cases, now using the 7-dimensional representation with highest weight $(1, 0, 0, 0)$ which is an extension of the 7-dimensional representation of L'_4 with image $\mathrm{SO}_7(k)$ (the weights are 0 and the orbit of the highest weight). The image of a long root element in L'_4 has two non-trivial Jordan blocks of size 2 in this representation. The rest of the argument is similar to the other cases.

We have shown that H is not contained in any (maximal) parabolic subgroup. \square

3. CHARACTER COMPUTATIONS

As in the introduction, let $p > 3$ be a prime, k be an algebraic closure of \mathbb{F}_p and $G = F_4(k)$ be a simple linear algebraic group with root system of type F_4 . Recall that we have fixed three conjugacy classes C_1 , C_2 and C_3 of G as follows. The class C_1 consists of involutions whose centralizer is a connected reductive subgroup with root system of type $A_1 + C_3$. Note that G is of simply-connected type and so all centralizers of semisimple elements are connected ([3, 3.5.6]). The class C_2 contains elements with Jordan decomposition $su = us$ where s is an involution with a reductive centralizer with root system of type B_4 and u is a long root element in the centralizer $C_G(s)$ of s . More precisely, $C_G(s)$ is isomorphic to the group $\mathrm{Spin}_9(k)$ and the image of u in the representations as $\mathrm{SO}_9(k)$ has Jordan block sizes $2^2 1^5$. The centralizer of u in $C_G(s)$, which is the centralizer $C_G(su)$, is connected ([12, 14.3]). The third class C_3 consists of the regular unipotent elements of G . Since we are in good characteristic for G the centralizer in G of $u \in C_3$ is also connected ([3, 5.6.1]).

Now we consider for each power q of p the finite group $F_4(q)$. Since our conjugacy classes C_1 , C_2 and C_3 contain elements in $F_4(p)$ and since these elements have connected centralizer in G it follows from the Lang-Steinberg theorem that C_1 , C_2 and C_3 intersect each $F_4(q)$ in a single $F_4(q)$ -conjugacy class.

Despite a lot of theory that is known about the ordinary characters of the groups $F_4(q)$ it is still impossible to compute their full character tables. However, using partial information about the character table we can work out the following result.

Theorem 3.1. *Let $X = V(C_1, C_2, C_3)$ be as before and $X(q)$ be the set of \mathbb{F}_q -rational points of X for any power q of p . There exists a positive constant c such that for all p and q :*

$$1 - \frac{c}{q} < \frac{|X(q)|}{|F_4(q)|} < 1 + \frac{c}{q}.$$

Remark. In particular $X(q)$ is not empty for large enough q . In section 4 we will show that in fact the quotient $|X(q)|/|F_4(q)|$ is precisely 1 for all q .

Proof. (of the theorem)

(1) Let $x \in C_1 \cap F_4(p)$, $y \in C_2 \cap F_4(p)$ and $z \in C_3 \cap F_4(p)$. The quantity $|X(q)|/|F_4(q)|$ can be computed as class structure constant by the following formula (see for example [15, I. Thm. 5.8]):

$$\frac{|X(q)|}{|F_4(q)|} = \frac{|F_4(q)|}{c_x(q)c_y(q)c_z(q)} \sum_{\chi \in \text{Irr}(F_4(q))} \frac{\chi(x)\chi(y)\chi(z)}{\chi(1)},$$

where $c_x(q)$, $c_y(q)$ and $c_z(q)$ are the centralizer orders of x, y, z , respectively, in $F_4(q)$.

The factor $|F_4(q)|/(c_x(q)c_y(q)c_z(q))$ is a quotient of two monic polynomials in q of the same degree, so it tends to 1 for growing q . It remains to show a lower and an upper bound as in the theorem for the sum in the formula.

(2) Since G has trivial (and hence connected) center we can use Lusztig's parameterization of the irreducible characters of $F_4(q)$ in [13, Ch.4]. Here, to each conjugacy class of semisimple elements in the dual group of $F_4(q)$, which is isomorphic to $F_4(q)$ itself, Lusztig associates a subset of the irreducible characters, which we now call a *Lusztig series*. For a semisimple element s of the dual group the corresponding Lusztig series is parameterized by some set which only depends on the twisted Lie type of the centralizer of s . We do not need the full details of this description because of the next two remarks.

(3) We only need to know character values of irreducible characters which are non-zero on all three classes C_1 , C_2 and C_3 . The characters which have non-zero value on class C_3 (regular unipotent elements) are called *semisimple characters*. Each Lusztig series contains exactly one semisimple character, see [3, 8.3, 8.4] (note that we use here our assumption that p is a good prime for G).

(4) Semisimple characters are uniform, which means that they are linear combinations of Deligne-Lusztig characters. An explicit description of this linear combination is given in [3, 8.4.6].

(5) The semisimple conjugacy classes of $F_4(q)$ (and its isomorphic dual group) were determined in [17]. But we need a slightly more precise description. We first describe representatives of the $F_4(q)$ -classes of centralizers of semisimple elements in the dual group (this does not depend on q) and then for each of them the elements in the center of this centralizer. We also (re)-compute the number of semisimple classes whose elements have centralizer in each class.

(6) We need representatives of the $F_4(q)$ -classes of maximal tori in G and parameterizations of their elements, this can be done as in (5). Furthermore, if T and T^* are dual maximal tori in G and its dual group, stable under a Frobenius morphism over \mathbb{F}_q , we need to associate to a pair (T^*, s) with $s \in T^*(q)$ an explicit linear character of $T(q)$. This is described in the proof of [4, 13.7]. Furthermore, we identify representatives of the semisimple parts of elements in our classes C_1 and C_2 in these tori.

(7) We compute the values of Deligne-Lusztig characters on the trivial class and on our classes C_1 , C_2 and C_3 via the character formula [3, 7.2.8]. In addition to (6) we need some values of Green functions for this computation. For the trivial class and C_1 these can be computed from certain torus orders, see [3, 7.5.1]. On the regular unipotent elements Green functions have value 1, see [3, 8.4.3]. And on the long root elements in groups of type B_4 they can be computed using [18].

(8) Now we can compute the values of all semisimple characters on the classes we consider as linear combinations of certain Deligne-Lusztig characters using (7), (6) and (4). We get parameterized descriptions of the values for all Lusztig series corresponding to semisimple elements s with a fixed class of centralizer. We call such a subset of semisimple characters a *semisimple character type*. These values are polynomials in q whose coefficients are sums of powers of -1 (the root of unity of order 2) where these powers depend on certain parameters which distinguish the characters within a character type.

For more details on such computations we refer to [2, Section 2] and [11]. We have used computer programs which are based on code provided by the CHEVIE package [6]. The results are a bit different according to the cases $q \equiv 1, 5, 7, 11 \pmod{12}$, so all computations must be done separately for each of these congruence classes of q modulo 12.

(9) In the statement of the theorem the 1 on the right hand side comes from the trivial character in the sum. To show that all other characters contribute something of absolute value less than a (big enough) constant times $1/q$, we can show this for each semisimple character type corresponding to non-trivial semisimple elements in the dual group separately (there are about 100 semisimple character types).

Let χ_s be the semisimple character corresponding to a semisimple element s in the dual group, and let n_s be the number of characters in the semisimple character type of s (n_s is also a polynomial evaluated at q). For most semisimple character types we find that the degrees as polynomials in q of $f_s := n_s \chi_s(x) \chi_s(y) \chi_s(z) |F_4(q)| / \chi_s(1)$ and of $|F_4(q)|$ are the same. So, just comparing the degrees of these polynomials is not good enough, we must show that at least the leading coefficients of the f_s sum up to zero when we sum over all s corresponding to a fixed semisimple character type.

We illustrate this with an example. Consider elements s which are regular elements in a maximal torus of order $(q+1)(q^3+q^2+q+1)$. These are parameterized by two integers $1 \leq m \leq q^3+q^2+q+1$ and $1 \leq n \leq q+1$ with the exception of $O(q^3)$ parameter pairs (which correspond to non-regular elements in that torus). The leading coefficient of $\chi_s(x) \chi_s(y) \chi_s(z) |F_4(q)| / \chi_s(1)$ is $((-1)^{n+m} + (-1)^n) q^{48}$. Since q is odd we see that the coefficients of q^{48} cancel out if we sum over all parameters m, n as above. Hence the complete summation over the characters in this semisimple character type can be bounded by a constant times q^{48+3} while $|F_4(q)| = q^{52} + O(q^{51})$. \square

4. PROOF OF THEOREM 1.1

Let k be an algebraic closure of \mathbb{F}_p , $p > 3$, and $G = F_4(k)$. Let $X = \{(x, y, z) \mid x \in C_1, y \in C_2, z \in C_3, xyz = 1\}$ be as before.

In Theorem 2.1 we have seen that the group generated by any triple in X contains a conjugate of $F_4(p)$. Therefore, the stabilizer of each triple must centralize a conjugate of $F_4(p)$, hence it is trivial (and connected). This shows that each G -orbit on X is regular.

Each triple in X is contained in a finite subgroup $F_4(q)$ for some power q of p (because $k = \overline{\mathbb{F}}_p$), and so its G -orbit is stable under all Frobenius morphisms of G over \mathbb{F}_{q^m} , $m \in \mathbb{N}$. It follows from the Lang-Steinberg theorem that the \mathbb{F}_{q^m} -rational points of such an orbit form one regular $F_4(q^m)$ -orbit.

In Theorem 3.1 we have computed an estimate for $|X(q)|/|F_4(q)|$ which shows that for all sufficiently large q the set $X(q)$ is not empty and consists of exactly one $F_4(q)$ -orbit. Hence X consists of a single G -orbit.

Now X is invariant under the Frobenius morphism of G over the prime field \mathbb{F}_p (because our classes C_i are defined over \mathbb{F}_p) and so over any \mathbb{F}_q for powers q of p . And since it is a single G -orbit we can apply again the Lang-Steinberg theorem and see that the set $X(q)$ of \mathbb{F}_q -rational points of X is not empty and is a single $F_4(q)$ -orbit. Using this for $q = p$ and Theorem 2.1 again a triple from $X(p)$ must generate $F_4(p)$. Therefore, all triples from X generate conjugates of $F_4(p)$.

REFERENCES

- [1] A. Borel, R. Friedman, J. Morgan, *Almost commuting elements in compact Lie groups*. Mem. Amer. Math. Soc. **157** (2002), no. 747.
- [2] O. BRUNAT, F. LÜBECK, On defining characteristic representations of finite reductive groups. J. Algebra **395** (2013), 121–141.
- [3] R. W. CARTER, *Finite Groups of Lie Type. Conjugacy Classes and Complex Characters*. Wiley Classics Library. John Wiley & Sons, Chichester, 1993.
- [4] F. DIGNE, J. MICHEL, *Representations of Finite Groups of Lie Type*. LMS Student Texts, **21**. Cambridge University Press, Cambridge, 1991.
- [5] W. FEIT, P. FONG Rational rigidity of $G_2(p)$ for any prime $p > 5$, Proceedings of the Rutgers group theory year, 1983–1984 (New Brunswick, N.J., 1983–1984), 323–326, Cambridge Univ. Press, Cambridge, 1985.
- [6] M. GECK, G. HISS, F. LÜBECK, G. MALLE, AND G. PFEIFFER, CHEVIE—a system for computing and processing generic character tables. Appl. Algebra Engrg. Comm. Comput. **7(3)** (1996), 175–210.
- [7] R. M. GURALNICK, G. MALLE, Rational rigidity for $E_8(p)$. Compos. Math. **150** (2014), 1679–1702.
- [8] J.-S. HUANG, J. YU, Klein four-subgroups of Lie algebra automorphisms. Pacific J. Math. **262** (2013), no. 2, 397–420.
- [9] C. KHARE, M. LARSEN, G. SAVIN, Functoriality and the inverse Galois problem. Compos. Math. **144** (2008), 541–564.
- [10] C. KHARE, M. LARSEN, G. SAVIN, Functoriality and the inverse Galois problem. II. Groups of type B_n and G_2 . Ann. Fac. Sci. Toulouse Math. (6) **19** (2010), 37–70.
- [11] F. LÜBECK, Charaktertafeln für die Gruppen $\mathrm{CSp}_6(q)$ mit ungeradem q und $\mathrm{Sp}_6(q)$ mit geradem q . Dissertation, Universität Heidelberg (1993).
- [12] G. LUSZTIG, Intersection cohomology on a reductive group. Invent. Math. **75** (1984), 205–272.
- [13] G. LUSZTIG, *Characters of reductive groups over a finite field*. Annals of Mathematics Studies **107**, Princeton University Press, 1984.
- [14] G. MALLE, Exceptional groups of Lie type as Galois groups. J. Reine Angew. Math. **392** (1988), 70–109.
- [15] G. MALLE, B. H. MATZAT, *Inverse Galois Theory*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 1999.
- [16] J. SAXL, G. M. SEITZ, Subgroups of algebraic groups containing regular unipotent elements. J. London Math. Soc. **55** (1997), 370–386.
- [17] T. SHOJI, The conjugacy classes of Chevalley groups of type (F_4) over finite fields of characteristic $p \neq 2$. J. Fac. Sci. Univ. Tokyo **21** (1974), 1–17.
- [18] T. SHOJI, Green functions of reductive groups over a finite field. Proc. Symp. Pure Math. **47** (1987), 289–301.
- [19] J. THOMPSON Rational rigidity of $G_2(5)$, Proceedings of the Rutgers group theory year, 1983–1984 (New Brunswick, N.J., 1983–1984), 321–322, Cambridge Univ. Press, Cambridge, 1985.
- [20] Z. YUN, Motives with exceptional Galois groups and the inverse Galois problem. Invent. Math. **196** (2014), no. 2, 267–337.
- [21] D. ZYWINA, The inverse Galois problem for $\mathrm{PSL}_2(\mathbb{F}_p)$, Preprint, arXiv:1303.3646v1.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF SOUTHERN CALIFORNIA, LOS ANGELES, CA 90089-2532, USA

E-mail address: `guralnic@usc.edu`

LEHRSTUHL D FÜR MATHEMATIK, RWTH AACHEN, PONTDRIESCH 14/16, 52064 AACHEN, GERMANY

E-mail address: `Frank.Luebeck@math.rwth-aachen.de`

BEIJING INTERNATIONAL CENTER FOR MATHEMATICAL RESEARCH, NO. 5 YIHEYUAN ROAD, BEIJING 100871, CHINA.

E-mail address: `junyu@math.pku.edu.cn`